

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

IN RE: CAPITAL ONE CONSUMER DATA
SECURITY BREACH LITIGATION

MDL No. 1:19md2915 (AJT/JFA)

This Document Relates to the Consumer Cases

**PLAINTIFFS' REPLY IN SUPPORT OF PLAINTIFFS'
MOTION TO COMPEL DISCOVERY FROM AMAZON DEFENDANTS**

Plaintiffs submit this Reply in Support of their Motion to Compel Discovery from Amazon Defendants ("Motion" or "Mot.") (Dkts. 454–456).

PRELIMINARY STATEMENT

On May 20, 2020, Defendants Amazon Web Services, Inc. ("AWS") and Amazon.com, Inc. (collectively, "Amazon") filed their Memorandum of Law in Opposition to Plaintiffs' Motion to Compel Discovery ("Opposition" or "Opp.") (Dkt. 472). In the Opposition, Amazon implicitly concede the discovery Plaintiffs seek is relevant to this litigation, but attempt to frame the scope of that discovery more narrowly than the rules dictate, and without carrying their hefty burden of proving with any detail that Plaintiffs' entitlement to this information is proportionately outweighed by any burden Amazon may undertake in responding thereto. Accordingly, the Court should find in Plaintiffs' favor and compel Amazon to respond to the discovery requests.

ARGUMENT

A. WAFs, SSRF and Open Reverse Proxy Attacks, and Overly Broad IAM Permissions is Relevant to Amazon's Knowledge of Potential Security Vulnerabilities

i. Capital One has not refuted the applicability of SSRF attacks to this case

Amazon contends SSRF was not at issue in the breach, [REDACTED]

[REDACTED] Amazon cites Mr.

Fisk's testimony in their Opposition, claiming [REDACTED]
[REDACTED] Opp. at 6 (emphasis in original). That exact cited
testimony [REDACTED] and is provided in full below:

[REDACTED]

(Doc. 472-1, Ex. A, at 102:7–16) (emphasis added). Mr. Fisk [REDACTED]
[REDACTED] Mr. Fisk testified [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] (Doc. 472-1, Ex. A, at 102:13–16) (emphasis added). Although this testimony [REDACTED]
[REDACTED] and does not eradicate Plaintiffs' theories of
liability and the applicability of SSRF to this case—especially concerning discovery.

And Amazon's selective citation to Mr. Fisk's testimony in an attempt to absolve itself
omits important facts implicating its liability. Indeed, Mr. Fisk also testified to [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Be that as it may, and even assuming Mr. Fisk had testified vociferously and unequivocally
to only what Amazon implies—and he did not—neither this Court nor Plaintiffs are required to
accept that testimony as undisputed fact. Importantly, Plaintiffs expect their expert(s) to establish

that an SSRF attack was at issue here, and, more to the point, Plaintiffs are already aware of multiple aspects of Capital One’s corporate representative testimony that is directly contradicted by documents already produced in this case and authored by Capital One employees. The actual facts in this case will be developed in the fulness of time and in the crucible of discovery; not by selected soundbites from a corporate designated witness in the *first* deposition taken in this case.

ii. The Information is abundantly relevant

Contrary to Amazon’s arguments, Plaintiffs’ requests for the Contested Discovery is anything but a fishing expedition. *See* Opp. at 3. Counter to this argument, Amazon concedes “Discovery from Amazon relevant to Plaintiffs’ claims in the representative complaint should focus on: (1) *what Amazon knew* and communicated with Capital One about the aspects of Capital One’s AWS account that Thompson exploited[.]” Opp. at 4 (emphasis added). As Amazon concedes, it is crucial to understand *what Amazon knew* concerning any WAFs, SSRF and open reverse proxy attacks, and overly broad IAM permissions, but Amazon curiously seeks to narrow the scope to what was communicated with Capital One—this improperly narrows the scope of permissible discovery Plaintiffs are entitled to take in this case. Also, Amazon concedes production of documents related to “IAM and security features available to customers” concern relevant areas of inquiry for Plaintiffs. Opp. at 5. Despite this concession that the arguably broader topic of what was available to customers is relevant, Amazon opposes Plaintiffs’ inquiry into the narrower topic of Amazon’s knowledge concerning whether overly broad IAM permissions contributed to prior data breaches or security incidents. These concessions recognize that the information Plaintiffs seek is relevant, yet contest the scope of Plaintiffs’ request extending beyond those involving Capital One.

Courts have routinely ruled that reasonably limited discovery concerning prior incidents is permissible if relevant to any matter raised in litigation. *See, e.g., Donovan v. Wal-Mart Stores,*

Inc., 2012 WL 3025877, *2 (D. S.C. July 24, 2012) (finding that occurrences and resolutions of similar incidents is discoverable); *United Oil Co., Inc. v. Parts Assoc., Inc.*, 227 F.R.D. 404 (D. Md. 2005) (compelling production of similar incidents in a products liability action); *Marks v. Global Mortgage Group, Inc.*, 218 F.R.D. 492, 497 (S.D. W. Va. 2003) (permitting discovery of similar transactions in lender liability litigation); *Bates v. Firestone Tire and Rubber Co., Inc.*, 83 F.R.D. 535 (D. S.C. 1979) (permitting discovery of manufacturer's knowledge of previous injuries or lawsuits involving specified product). Indeed, the scope is not limited to local geographic or short temporal scopes. *See, e.g., Pham v. Wal-Mart Stores, Inc.*, No. 2:11-cv-01148-KJD-GWF, 2011 WL 5508832 (D. Nev. Nov. 9, 2011) (permitting nationwide discovery of similar accidents involving mattress display during a five-year period); *Fears v. Wal-Mart Stores, Inc.*, No. Civ.A. 99-2515-JWL, 2000 WL 1679418 (D. Kan. Oct. 13, 2000) (permitting nationwide discovery of similar accidents resulting from falling merchandise during a five-year period).

Plaintiffs' position is no different than the cases collected above: Plaintiffs do not seek information related to any security vulnerability experienced by any Amazon customer from Amazon's inception to the present day. Instead, Plaintiffs seek targeted discovery related to specific security vulnerabilities during the period in which Capital One has been using Amazon's services. By way of example, during meet and confers Amazon has taken the position that it is essentially a landlord: it provided a space for Capital One to store its customers' data. If, however, Amazon (as a landlord) knew that the locks to the property were susceptible to simple lockpicking or that burglars had robbed the property by sneaking through a window that had no locks (e.g., exploiting misconfigured WAFs, SSRF and open reverse proxy attacks, or overly broad IAM permissions), that information is vital to the determination of whether the property was provided in a safe and secure condition in the first place. Whether that information was communicated to

the tenant is obviously important, but the focus cannot be limited to just those communications because that would encourage lack of candor and insulate Amazon from liability simply by its own silence.

B. The Financial Benefits Amazon Received as a Condition of Partnering with Capital One is Relevant to Plaintiffs’ Unjust Enrichment and Disgorgement Claims

Amazon is plainly wrong that financial information is not relevant to any element of Plaintiffs’ claims: one of the driving questions of this litigation is why Defendants were retaining decades-worth of data—stretching back to credit applications from 2005—and storing it in the AWS cloud. Plaintiffs allege that Capital One’s migration to AWS “allowed Capital One to use Amazon’s data scientists and artificial intelligence tools to analyze the trove of customer data it collected from credit applicants,” and that the “strategy was an aggressive move into uncharted territory for a major bank.” (Doc. 354, ¶¶ 40–41). “AWS’s servers facilitate machine learning by allowing large amounts of data to be collected in a common pool, which is segmented into folders. This AWS configuration allows for different web applications to draw from a vast collection of data” (*Id.* ¶ 47).

PII from tens of millions of consumers spanning nearly 15 years is truly a treasure trove of information; a trove Amazon may also have been mining for its own financial gain—leveraging its data scientists, artificial intelligence tools, and machine learning, as alleged in the Complaint and set out above. Such information is clearly relevant to Plaintiffs’ Unjust Enrichment claim, amongst others: if Amazon was financially benefiting from using Plaintiffs’ PII, while also failing to adequately protect it, retaining such benefits would arguably be inequitable. *See e.g., In re Facebook, Inc. Internet Tracking Litig.*, --- F.3d ---, 2020 WL 1807978, at *6 (9th Cir. Apr. 9, 2020) (holding plaintiffs’ “stake in unjustly earned profits [from the collection and use of consumers’ browsing histories] exists regardless of whether an individual planned to sell his or

her data or whether the individual’s data is made less valuable”); *Kokesh v. S.E.C.*, 137 S. Ct. 1635, 1640 (2017) (“Disgorgement requires that the defendant give up ‘those gains . . . properly attributable to the defendant’s interference with the claimant’s legally protected rights.’”) (quoting Restatement (Third) of Restitution and Unjust Enrichment § 51, Comment a, p. 204 (2010)).

Accordingly, Plaintiffs seek discovery of information from Amazon regarding whether it financially benefited from the use or manipulation of Plaintiffs’ PII stored by Capital One on Amazon’s cloud. Accordingly, Amazon’s argument that “[f]inancial benefit cannot establish duty, proximate causation, or injury” (Opp. at 9) is misplaced; Plaintiffs have alleged more than just negligence claims, and whether Amazon financially benefited from Plaintiffs’ PII—which Defendants failed to protect—is relevant to this case.

C. Amazon Has Failed to Carry its Burden of Demonstrating the Contested Discovery is Burdensome, Overly Broad, or Otherwise Not Proportional to the Needs of this Case

A court is permitted to limit discovery “if it finds that ‘the burden or expense of the proposed discovery *outweighs its likely benefit*, taking into account the needs of the case, the amount in controversy, the parties’ resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues.’” *Stoney Glen, LLC v. Southern Bank and Trust Co.*, 2013 WL 5514293, at *3 (E.D. Va. Oct. 2, 2013) (Payne, J.) (quoting Fed. R. Civ. P. 26(b)(2)(iii)) (emphasis added). Importantly, “[t]o prevail on the grounds of burdensomeness or breadth, the objecting party must do more to carry its burden than make conclusory and unsubstantiated arguments.” *Id.* (citing *Converting v. United States Dep’t of Justice*, 565 F.Supp.2d 10, 14 (D.D.C. 2008); *Cory v. Aztec Steel Bldg., Inc.*, 225 F.R.D. 667, 672 (D. Kan. 2005) (the party opposing discovery on the ground of burdensomeness must submit detailed facts regarding the anticipated time and expense involved in responding to the discovery which justifies the objection)).

Instead of permitting Plaintiffs to explore whether Amazon has any knowledge of improperly configured WAFs, SSRF and open reverse proxy attacks, and overly broad IAM permissions—and if so, the details of that knowledge—Amazon instead implores the Court to foreclose this inquiry altogether because it *may* require Amazon to take on a burden for that search, even though Amazon simply has failed to carry its burden of proving the burdensomeness or breadth outweigh Plaintiffs’ entitlement to the Contested Amazon Discovery. In their response, Amazon tacitly acknowledges no preliminary search for the requested information has been made in any manner whatsoever. *See Opp.*, at 1 (“Amazon’s knowledge (*if any*) of how other customers configure their own AWS environments is of no relevance or value in this case....”) (emphasis added). Instead, Amazon focuses its argument on the number of clients it services and the anticipated production concerning Capital One.

For obvious reasons, Amazon eschews responding to or otherwise refuting the proportionality factors Plaintiffs enumerated and argued in the Motion—those factors weigh heavily in Plaintiffs’ favor. *Mot.* at 8 (citing *BASF Plant Sci., LP v. Commonwealth Sci. and Indus. Research Org.*, No. 2:17-cv-503, 2019 WL 8108060 (E.D. Va. July 3, 2019) (Morgan, J.)). This is one of the largest data breaches in history and concerns some of the most sensitive information a person can provide to a company; Amazon is in a substantially better position to search for and provide this information; Amazon has the resources to gather this information; and there is no prejudice or undue hardship to Amazon or even the non-parties in this case; the parties are subject to a comprehensive and thoroughly litigated and negotiated protective order, and the information sought would undoubtedly be subject to that order. *Mot.* at 13. Although Amazon argues it has numerous customers, Amazon presents no evidence concerning what subset of customers could be subject to these discovery requests, any anticipated number of documents, or any other details

required for this Court to make an informed decision regarding the proportionality of the request to this litigation. Instead, Amazon avers “The burden on Amazon of conducting such an inquiry would be enormous, and virtually impossible to complete on the discovery timeframes in this case.” (Doc. 472-3, ¶ 4).

Amazon’s reliance on *E.I. Du Pont Nemours and Co. v. Kolon Ind., Inc.*, is misplaced, and, in fact, inures to Plaintiffs’ benefit. In *Kolon*, Du Pont sought information from Kolon related to accounts receivable and other financial information concerning post-verdict collections. No. 3:09-cv-058, 2012 WL 1664250, at *2 (E.D. Va. May 11, 2012). The *Kolon* court analyzed prior discovery production that Kolon provided to Du Pont—including “Kolon’s 25 largest U.S. and worldwide customers and charts of outstanding Accounts Receivable.” *Id.* The *Kolon* court found that “the identity of a customer *is relevant when Kolon holds a receivable from that customer or the customer otherwise holds Kolon assets*. The motion to compel is granted to the extent that it seeks that information. [...] The motion to compel additional customer information will be denied *to the extent that it seeks such additional information*” *Id.* (emphasis added).

Here, Plaintiffs have not requested all information from all of Amazon’s customers related to security (*i.e.*, all customer information like in *Kolon*); rather, Plaintiffs requested discrete and detailed information specifically related to the security vulnerabilities at issue in this case (*i.e.*, all customer information for which debt is owed like in *Kolon*). That Amazon has identified two million documents relevant to *all of Plaintiffs’ discovery requests* is a false equivalency, which does not dictate that similar efforts related to Amazon’s knowledge of issues with misconfigured WAFs, SSRF and open reverse proxy attacks, or overly broad IAM permissions outside of the Capital One context would result in the same volume of documents or work to be performed. Plaintiff made these requests in January, yet as of May 20, 2020—nearly four months later—

Amazon appears not to have even undertaken a preliminary review of potentially relevant documents for these requests, and instead asserted tenuous objections based on alleged burdensomeness.

CONCLUSION

For all the reasons set forth above and in their Motion, Plaintiffs request that the Court grant their Motion to Compel and issue an order compelling Amazon to respond to the interrogatories and requests for production, produce a competent and prepared witness on the identified topics consistent with Rule 30(b)(6), and any other relief this Court deems proper.

Dated: May 21, 2020.

Respectfully Submitted,

/s/ Steven T. Webster
Steven T. Webster (VSB No. 31975)
WEBSTER BOOK LLP
300 N. Washington Street, Suite 404
Alexandria, Virginia 22314
Tel: (888) 987-9991
swebster@websterbook.com

Plaintiffs' Local Counsel

Norman E. Siegel
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, MO 64112
Tel: (816) 714-7100
siegel@stuevesiegel.com

Karen Hanson Riebel
**LOCKRIDGE GRINDAL NAUEN,
P.L.L.P**
100 Washington Avenue South, Suite 200
Minneapolis, MN 55401
Tel: (612) 339-6900
khriebel@locklaw.com

John A. Yanchunis
**MORGAN & MORGAN COMPLEX
LITIGATION GROUP**

201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel: (813) 223-5505
jyanchunis@ForThePeople.com

Plaintiffs' Co-Lead Counsel

CERTIFICATE OF SERVICE

I hereby certify that on May 21, 2020, I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system, which will send notice of electronic filing to all counsel of record.

/s/ Steven T. Webster
Steven T. Webster (VSB No. 31975)
WEBSTER BOOK LLP